ELECTRONIC MONEY LAUNDERING:
An Environmental Scan

Department of Justice Canada

Solicitor General Canada

October 1998

"Jurisdictions should... determine the money laundering threats inherent in new or developing technologies, such as smart cards, electronic banking, etc., and take necessary measures to prevent their use in money laundering schemes. *Financial Action Task Force, 1996."*

This environmental scan is not meant to be all inclusive but rather to stimulate thought on emerging criminal justice issues. It does not, represent the policy of the Solicitor General Canada, the Government of Canada, or any other Federal Government Agency or Department

TABLE OF CONTENTS

PREFACE ii

EXECUTIVE SUMMARY iii

1.0 MONEY LAUNDERING 1
- **1.1 What is Money Laundering?** 1
- **1.2 Effects of Money Laundering** 2
- **1.3 Strategies and Initiatives** 2

2.0 ELECTRONIC MONEY 4
- **2.1 What is Electronic Money?** 4
- **2.2 The Scope of Electronic Money** 5
- **2.3 The Potential for Electronic-Money Laundering** 7

3.0 CHALLENGES FOR CRIMINAL JUSTICE 9
- **3.1 Legislative and Regulatory Issues** 9
- **3.2 Policing and Law Enforcement Issues** 10

4.0 INTERNATIONAL COOPERATION 12

5.0 CONCLUSION 15

BIBLIOGRAPHY 16

APPENDICES:

Appendix I: How E-money Works 25
Appendix II: Cryptography and Electronic Commerce 27
Appendix III: Payment Systems Attributes 28
Appendix IV: Survey of G-10 Policies on Electronic Money 30
Appendix V: FATF Recommendations 36

104-05955/

PREFACE

This environmental scan is part of a continued partnership between the Department of Justice Canada and the Solicitor General Canada. *Electronic Money Laundering* was co-authored by Jasmine Brown and Austin Lawrence of the Department of Justice Canada, and Darryl Sitka and Raffaele Fasiolo of the Solicitor General Canada.

This scan begins by defining electronic money and looks at its effects; it then defines electronic money, its scope, and the potential for electronic money laundering. The challenges for the criminal justice system are investigated; the report concludes with looking at the importance of international co-operation.

EXECUTIVE SUMMARY

This scan was produced jointly by Solicitor General Canada and the Department of Justice Canada.

Financial systems are emerging in which economic value is represented by electronic patterns. This 'electronic cash' or 'e-money' can be exchanged through the use of 'smart cards' or over the Internet. E-money is expected to work just like paper money, but without the risks, inconvenience and costs involved in handling, administering and safeguarding actual physical currency.

The explosion of e-money technology raises a number of policy issues, one of which is money laundering. Any crime that generates significant profits — extortion, drug trafficking, arms smuggling and some kinds of white-collar crime — may involve attempts at money laundering.

E-money may prove to be attractive to money launderers for two main reasons:
Electronic transactions may become *untraceable* and are *incredibly mobile*. E-money transactions can easily be anonymous and may not leave a traditional audit trail. E-money systems also offer instantaneous transfer of funds with effectively no jurisdictional restrictions.

Given these challenges, new legislative and regulatory action, investigative and enforcement techniques, and most important, enhanced international cooperation may be needed to prevent, detect and apprehend e-money launderers. These may need to cover many areas:

- domestic measures, to give law enforcement agencies more effective tools;
- training, both for law enforcement agencies and in the financial sector, including financial regulators;
- information sharing and retention, in Canada and internationally; and
- secrecy laws, to hinder money laundering without hindering legitimate transactions.

1.0 MONEY LAUNDERING

Before we can grasp the potential impact of electronic-money technologies on money laundering, we must first understand how money laundering works.

1.1 What is Money Laundering?

Money laundering is the conversion or transfer of property, knowing that such property is derived from criminal activity, for the purpose of concealing the illicit nature and origin of the property from government authorities.

Any crime that generates significant profit — extortion, drug trafficking, arms smuggling and some kinds of white collar-crime — may create a "need" for money laundering.

How is money laundered? Typically, by moving it from one country to another (physically or electronically) and obscuring its origin through complicated financial transactions. According to the Financial Action Task Force (FATF), estimates of the amount of money laundered annually worldwide from the illicit drug trade alone range between $US 300 billion and $US 500 billion. The inclusion of laundered illicit funds from economic and other non-drug crime could potentially double these figures (Porteous, 1998).

Money Laundering costs our economy billions of dollars.

The size of the illicit drug market in Canada has been estimated to be between $7 billion to $10 billion. Expert opinion holds that between 50-70% of drug sales revenues are available for laundering and subsequent investment. Assuming in addition, as has been argued, that 50-70% of the funds laundered in Canada are derived from illicit drugs, then the amount of illicit funds laundered in Canada per year is between $5 billion and $14 billion (Porteous, 1998).

Non-drug money laundering schemes are usually related to "enterprise crimes" such as the smuggling of contraband alcohol, tobacco, pornography and firearms, illegal immigration rackets (people smuggling) as well as illegal gambling and prostitution.

Large-scale tax evasion in the underground economy also leads to money laundering, with perpetrators looking for ways to hide their revenues here in Canada or transfer them offshore.

Traditional methods for laundering funds include the use of shell corporations, offshore financial havens and cash-only businesses, and the abuse of certain financial services offered by banks and other deposit-taking institutions. Emerging markets (including the formal securities, insurance and money-changing sectors) are also increasingly becoming the venue for large-scale money laundering.

A significant amount of hard currency (cash, bonds, stock certificates) is physically transported across the Canada-US border by passenger couriers, as well as in freight. Electronic transmission of funds (wire transfers) is on the rise and the use of the Internet is an increasing concern.

1.2 Effects of Money Laundering

Money laundering has far-reaching consequences:

- **It makes crime pay.** It allows drug traffickers, smugglers and other criminals to expand their operations. This drives up the cost of law enforcement and health care (e.g., treatment of drug addictions).

- It has the potential to **undermine the financial community** because of the sheer magnitude of the sums involved. The potential for corruption increases with the vast amounts of illegally obtained money in circulation.

- Laundering **diminishes government tax revenue** and therefore indirectly harms honest taxpayers and reduces legitimate job opportunities.

- Perceived ease of entry to our country **attracts an undesirable element** across our borders, degrading our quality of life and raising concerns about our national security.

1.3 Strategies and Initiatives

Money laundering affects all Canadians from coast-to-coast, on our streets and in our communities.

A number of steps are being taken in Canada and around the world to counter money laundering. These include: strong national leadership, new legislation, regulations and financial policies, international cooperation, and border control. We will discuss some of the key current strategies and initiatives.

Canada has implemented **new legislation and regulations** targeting money laundering. These include changes to the *Criminal Code* to criminalize money laundering and the introduction of record-keeping legislation to facilitate investigations and prosecutions.

The recent amendments to the Code introduced by Bill C-95 gave police, prosecutors and courts a range of new powers to use in dealing with organized crime. Also, legislative amendments dealing with the creation of a mandatory suspicious transaction reporting system and cross-border controls are being considered.

To combat the movement of illegal funds across Canada's international border, Customs officers could be given increased powers to search for and detain suspicious currency and other monetary instruments. Although Customs does have the legal authority to search and detain suspicious

goods, currency is not included under the definition of goods. Amendments to the legislation to rectify this situation are being considered.

Canada could also consider establishing a **central authority** to oversee most aspects of the enhanced anti-money laundering initiatives. For now, a National Coordinating and five Regional Coordinating Committees of police and other officials meet regularly to identify best practices and share information, bringing a multi-disciplinary approach to the fight against organized crime.

The Government is developing tougher laws and controls to combat money laundering.

Canada is **working closely with other countries** to improve exchanges of information and to develop strategies related to tax havens and tax jurisdictions where there are bank secrecy laws. This work takes place in formal settings like the Organization for Economic Cooperation and Development, the Pacific Association of Tax Administrators, in bilateral discussions with treaty partners, and through information exchange.

Canada also actively participates in the G-7's Financial Action Task Force on money laundering, the P-8 Working Group on Transnational Organized Crime, the Inter-American Drug Abuse Control Commission, the Cross Border Crime Forum, and various other organizations dedicated to fighting finance-related organized crimes. Discussions are also taking place within the UN Crime Prevention and Criminal Justice Commission on the creation of an international instrument on transnational organized crime.

Memoranda of Understanding and Mutual Legal Assistance Treaties can be negotiated to ensure an effective exchange of information, as well as equitable asset-sharing arrangements.

The machinery already exists to fight traditional money laundering, but new approaches may be needed to deal with the special threat of *electronic* money laundering.

2.0 ELECTRONIC MONEY

2.1 What is Electronic Money?

By its decentralized, distributive nature, electronic money has the same potential for transforming economic structure as personal computers did for overhauling management and communications structure. ***Birch and McEvoy, 1996***

Financial systems are emerging which allow economic value to be represented digitally by electronic patterns. This 'electronic money', or e-money, can be exchanged through the use of 'smart cards' or over the Internet.

Unlike stored value cards, e-money can pass immediately between the two transacting on-line parties, without the need for an intermediary (e.g., e-cash by DigiCash Inc.).

E-money is ultimately expected to work just like paper money, without the risk, inconvenience and cost associated with handling, administering and safeguarding traditional currency.

(For a detailed explanation of how e-money works, see Appendix I.)

A bewildering variety of electronic payment systems is currently being developed around the world. Given the constant changes to these systems, it would not be practical to launch into a technical discussion on how they work.

E-money will transform our economic structure.

Interested readers may consult some of the many references in the bibliography. This section simply defines the nature and scope of e-money and how it relates to the threat of money laundering.

As technology has progressed, so too have payment systems. E-money is being introduced as the latest method of exchanging value. But governments have to be ready to react to the novel opportunities as well as the threats posed by this new form of currency.

The electronic exchange of money is by no means a brand new invention. Banks and other financial institutions have been using computers to deal with one another for quite some time.

In the United States, in terms of the *volume* of dollars exchanged, the computer-based Fedwire and Clearing House Interbank Payments System (or CHIPS) together account for 90% of all transactions. These systems are used mainly by large financial institutions.

On the other hand, if we're counting by the *number of individual transactions*, 90% are still made by cash or cheque. These are small-scale transactions involving individuals. These US patterns also apply to Canada.

Advances in three technological areas have made the widespread use of electronic cash economically viable, spurring interest in e-money. These advances are:

- reliable, quick networked communications with a low cost per transaction;
- better computer technology, allowing for the mass production of computer chip cards; and
- powerful public domain cryptography, to help ensure privacy and prevent fraud (see Appendix II for more on cryptography and electronic commerce).

What is revolutionary about the electronic cash systems currently being developed is that they are designed to mimic physical cash. This means they are strategically positioned to claim a large part of the small transaction market that accounts for the bulk of transactions. Electronic cash will affect society more than past electronic commerce advances because it will affect, and be affected by, the lives of ordinary people. (See Appendix III for a comparison of current payment systems.)

2.2 The Scope of Electronic Money

The actual level of commerce on the Internet is still modest by any standards. Unofficial estimates suggest there is only about $100 million to $200 million in annual transactions on the Internet at this time (US Department of the Treasury Conference, 1996). However, some people expect the value of Internet transactions alone (not smart cards) to skyrocket to roughly $10 billion by the year 2000.

Although commerce on the Internet is still fairly weak, e-money technology may be poised to take off. An industry trade magazine, *Smart Cards*, says "it is estimated that by 2001, over 100 billion transactions will be consummated using a smart card" (Cherneff *et al.*, 1996).

The hardware that will permit deep market penetration of the home-based e-money market is well on its way. Microsoft, Hewlett-Packard and Gemplus, for example, are already producing personal computer keyboards that will be able to read smart cards. AT&T plans to convert its public phones to operate by smart card. Mondex and Digi-Cash are testing smart card pilot projects around the world. Even the US government is moving toward implementing e-money systems; it is examining the feasibility of introducing 'paperless' benefit payments by 1999, using Electronic Benefit Transfer (EBT).

Ultimately, consumer and business acceptance of e-money will determine the extent to which it is used. Some of the possible benefits of e-money to consumers include:

- faster, more efficient transactions;
- less need to carry pocket money;
- loyalty and frequent user plans;
- automatic personal financial record-keeping;
- possible financial anonymity;
- possible security from theft;

- access to electronic commerce; and
- more personalized banking services and instruments.

The potential benefits of e-money to business are extensive. They include:

- instant transactions;
- substantial cost savings because of the reduction in the physical handling of currency;
- easier collection of marketing information on customers; and
- promotion of 'free banking'.

Traditionally, the two most important constraints on trade were time and distance. E-money systems effectively erase both. They will almost certainly help to globalize trade.

However, a number of barriers may halt or slow the widespread acceptance of e-money if they are not overcome. These include:

- for the operator, the cost of installing the technological infrastructure may be substantial;

- competing e-money systems will have to be compatible and integrated with current methods of payment;

- the cost of using the system will have to be kept lower than the cost of using current payment systems;

- the risk of losing cards and their charged value could intimidate some consumers;

- because security is a major concern, full convertibility, receipted transactions and high levels of security may all become features of e-money systems; and

- privacy of personal information will also be an important issue.

Solutions will probably be found to all these problems. All things considered, it seems likely that e-money will be an important part of everyday life in the very near future.

2.3 The Potential for E-money Laundering

What does e-money mean for the money launderer?

> The abuse of e-money by money launderers is a significant threat.

E-money laundering is thought to be negligible, for now:

> To date, G-10 countries have not seen evidence of this activity in connection with electronic money products; if such products come to be used on a large scale, it is conceivable that criminals may seek to explore their potential for transferring illicit funds. (Group of Ten, 1997).

Indeed, criminals are always looking for "a new type of detergent which allows for cleaner laundry" (Bortner, 1996). They have been quick to exploit each new method of financial transfer. In the 1980s and 1990s wire transfers became a popular method for moving money in both the legal and illegal sectors. By 2000 we may see the same situation with e-money. The abuse of e-money by money launderers may become a significant problem in the future because e-money systems will be attractive to money launderers for two reasons:

- transactions may become untraceable; and
- transactions are incredibly mobile.

Untraceability

> E-money systems may provide Organized Crime with untraceable, mobile wealth.

The use of e-money systems will mean fewer face-to-face financial transactions. The anonymity of e-money will make "knowing your customer" much more difficult.

E-money systems also allow the parties to the transaction to deal with each other directly, without the assistance of a regulated financial institution. Thus, there may not be a traditional audit trail.

Mobility

Hypothetically, e-money could come from anywhere in the world, and be sent anywhere in the world. Thus, e-money systems may offer instantaneous transfer of funds over a network that, in effect, is not subject to any jurisdictional restrictions.

The problem may be illustrated by separating the process of money laundering into three basic steps — placement, layering and integration — and then comparing traditional money laundering systems with cyber-systems.

The first step in money laundering is the physical disposal of cash. Traditionally, *placement* might be accomplished by depositing the cash in domestic banks or other kinds of financial institutions. Or the cash might be smuggled across borders for deposit in foreign accounts, or

used to buy high-value goods, such as artwork, airplanes, or precious metals and gems, that can then be resold with payment by cheque or bank transfer.

With e-money laundering, cash may be deposited into an unregulated financial institution. Placement may be easily achieved using a smart card or personal computer to buy foreign currency, goods, etc. Powerful encryption may be used to guarantee the anonymity of e-money transactions.

The second step, *layering*, involves working through complex layers of financial transactions to distance the illicit proceeds from their source and disguise the audit trail. This phase traditionally involves such transactions as the wire transfer of deposited cash, the conversion of deposited cash into monetary instruments (e.g., bonds, stocks, travelers' cheques), the resale of high-value goods and monetary instruments, and investment in real estate and legitimate businesses, particularly in the leisure and tourism industries. Shell companies, typically registered in offshore havens, are a popular device in the traditional layering phase. These companies, whose directors are often local attorneys acting as nominees, protect the identity of the real owners. These owners also benefit from restrictive bank secrecy laws and attorney-client privilege. In an electronic-money system, layering can be done through a personal computer. There is usually no audit trail. In addition, e-money systems allow for instantaneous transfer of funds over a system that, in effect, has no borders.

The last step is to make the wealth derived from crime appear legitimate. Traditionally, *integration* might involve any number of techniques, including using front companies to "lend" the money back to the owner or using funds on deposit in foreign financial institutions as security for domestic loans. Another common technique is over-invoicing, or producing false invoices for goods sold — or supposedly sold — across borders.

In e-money laundering the criminal may be able to achieve integration by using a personal computer to pay for investments or to buy an asset, without having to call on the services of an intermediary financial institution.

In short, the temptation of electronic forms of money for the criminal may be the potential for untraceable, mobile wealth.

3.0 CHALLENGES FOR CRIMINAL JUSTICE

3.1 Legislative and Regulatory Issues

Money laundering is only one of the many complex legislative issues that arise from the advent of e-money. As a specific form of computer-related economic crime, e-money laundering rests at the intersection of several different branches of law: commercial, privacy, computer, banking, intellectual property and criminal law. Exactly what the legal ramifications of this new technology will be has yet to be determined.

Current laws and regulations require businesses and consumers to provide information to enable government to combat certain financial crimes. How such laws apply to electronic payment systems is not clear.

Existing legislation and regulation may need to be modified.

The general attitude of regulatory authorities toward e-money has been to "let the market work it out." Because the pace of technological innovation is so rapid, institutional authorities have been reluctant to create new regulations to govern e-money before it is clear what form e-money, and its use, will take.

Even so, some countries have already begun to modify existing legislation so that it covers e-money. Europe has thus far leaned more toward government regulation and centralized control of e-money than has North America. (See Appendix IV for a survey of policies on e-money in the G-10 nations).

- Some US states have begun to apply money transmitter regulations to e-money providers.

- The US federal government has also modified the classifications in its *Electronic Fund Transfer Act* to account for on-line and off-line e-money.

- A proposed amendment to the banking law in Germany would include the transfer of e-money in the catalogue of banking transactions and, therefore, establish a basic principle of limiting the issuing of electronic payment methods to banks.

Canada has adopted a "wait and see" strategy in regard to e-money legislation. Current efforts are focused on communication between government and the businesses with e-money interests, and liaison with other governments.

Major legislation in Canada that may be relevant to e-money laundering includes:

- the *Proceeds of Crime Act* and its Regulations;
- the *Bank Act* and its Regulations; and

- Chapter C-46 of the *Criminal Code* (especially section 462.31 "Laundering Proceeds of Crime").

In short, governments have concentrated on research, networking and supervision of the emerging e-money sector.

3.2 Policing and Law Enforcement Issues

As e-money systems develop, governments may need to identify the additional legislative and regulatory measures that may be needed to combat money laundering and other financial crimes involving these systems. Police may have to develop new techniques to deal with on-line crime. Even so, it is likely that laws and regulations will always lag behind technological advances, and criminals will continue to exploit technology and try to stay one step ahead of the law.

The potential for abuse of e-money systems by organized crime, money launderers and other financial criminals could be significant. Because e-money could lead to untraceable transactions and offer unprecedented mobility both in terms of speed of transfer and absence of borders, it could create new enforcement challenges:

- In dealing with a paperless payment system with anonymous users, authorities will have fewer opportunities to use traditional techniques such as analyses of financial documents and surveillance of those suspected of financial crimes.

- Without an audit trail, it will be much more difficult for enforcement agencies to deter, detect and investigate illegal e-money activities.

- Instantaneous transactions further hinder detection, surveillance and apprehension. For example, once a digital credit is established, it may be used for any transaction. With the exception of the user's telephone bill, there will be no record of this transaction, which will typically be protected from detection by a key encryption system. Even the telephone record may not be available if a 1-900 masking system is used. Thus, investigations may become more costly and difficult.

Police may have to develop new detection, surveillance and investigative methods.

- Transactions without borders could confuse the issue of jurisdiction. If you don't know *where* a crime occurred, how do you decide *who* should investigate or prosecute it?

Evaluation of these issues will necessarily depend on the particulars of electronic payment systems and electronic cash products. For example, current smart-card systems like Mondex generate audit trails and limit the maximum value that a card may hold at any time. Reports from countries where these cards are used suggest that criminal interest in these cards is low (US Department of the Treasury Conference, 1996). However, law enforcement bodies are concerned

about potential developments in e-money systems that may permit anonymous, auditless, instantaneous transactions across borders. They may have to develop new detection, surveillance and investigative methods to prevent abuse of electronic payment systems by money launderers.

4.0 INTERNATIONAL COOPERATION

The single-most important weapon in the fight against e-money laundering is international cooperation. Because e-money is borderless, anti-laundering legislation, regulation, and investigative and enforcement techniques will be only as good as the weakest link in the international chain.

Governments have been working together to fight money laundering for the last 15 years or so. The main international agreements addressing money laundering are the 1988 UN *Vienna Convention* and the 1990 Council of Europe Convention.

Investigative and enforcement techniques will be only as good as the weakest link in the international chain.

The role of financial institutions in preventing and detecting money laundering has been the subject of reviews conducted by the Basle Committee on Banking Supervision, the European Union and the International Organization of Securities Commissions. Major international bodies, including the Financial Action Task Force (FATF) and the G-7/P-8 (Lyon Group), are trying to guide law enforcement agencies in preventing, detecting and apprehending money launderers.

The FATF is the main international body engaged in continuous, comprehensive efforts to define policy and to promote countermeasures against money laundering. Canada is an active member of the Task Force. The FATF has adopted 40 comprehensive recommendations covering areas such as: customer identification; minimum standards of record-keeping; cooperation among banks, supervisory and law enforcement agencies; and reporting of suspicious transactions. (For the complete set of FATF recommendations, see Appendix V.)

The Lyon Group focuses on legal mechanisms to fight financial crimes, especially money laundering. Specifically, a high-tech subgroup has been exploring issues involved in locating and identifying computer criminals in networked and wireless environments, and in collecting and sharing evidence, including situations in which transborder searches are necessary.

The following are highlights of some of the most pertinent recommendations from these groups:

Domestic Measures

- Ensure that appropriate mutual legal assistance mechanisms, including treaties, are in place to provide for compulsory production of records by financial institutions and other forms of assistance.

- Enable law enforcement authorities to identify, freeze, and/or confiscate proceeds or the methods used in the commission of any financial crime.

- Improve customer identification and record-keeping requirements to facilitate the identification and reporting of suspicious transactions and the detection and prosecution of money launderers.

- Enact legislation creating criminal liability for corporate entities.

- Encourage all countries to treat serious financial crimes as extraditable offences.

Training and Education

- Establish international training programs to assist governments in developing effective financial crimes enforcement operations and to foster cooperation among law enforcement agencies.

- Provide appropriate training within the financial industry, leading to the identification of systemic weaknesses and the development of solutions.

- Provide training for financial regulators and their examiners to improve their ability to detect financial crimes. Develop training programs within financial institutions to improve employees' ability to detect and prevent financial crimes, and address changing record-keeping and reporting requirements.

Information Sharing and Retention

- Enhance Interpol's existing efforts to share intelligence in regard to international financial crime. Interpol should consider establishing a sub-unit for financial crimes.

- Evaluate existing mutual legal assistance mechanisms to determine whether further efforts are required to combat financial crimes.

- Promote the development of international multi-agency task forces to investigate financial crimes.

- Require financial institutions to keep records on domestic and international transactions for five years or more.

Secrecy Laws

- Review secrecy laws to determine the need for legislative, regulatory or other actions to facilitate the sharing of financial institution records and related information between law enforcement agencies and regulatory authorities, and among governments.

It is too early to tell whether, in the long run, e-money will attract money launderers. To date, most G-10 countries have *not* seen the need to develop new legislation, enforcement policies or formal coordinating mechanisms specifically addressing e-money. In fact, they have confined their efforts so far to monitoring the situation and keeping in touch with the developers of e-money systems.

5.0 CONCLUSION

Canada's success in the 21st century will depend on our ability to participate in the global knowledge-based economy. The Government of Canada, in partnership with the private sector and other levels of government, is undertaking many initiatives to ensure this success. This partnership will help Canada benefit from the economic growth that will result from an intelligent approach to electronic commerce. But the electronic marketplace will have to be governed by a clear set of rules, so that corporations, institutions and individuals can have confidence in doing business electronically. Ensuring the safety and reliability of the system will be crucial.

Money laundering by traditional methods is already a serious problem. New e-money technologies have the potential to make money laundering much more widespread, as well as complicating efforts to fight it.

Transnational criminals could benefit tremendously from e-money technologies.

The requirement that electronic payments begin and/or end in a financial institution (to ensure that transaction amounts stay small and actors identifiable) may be weakened by increasing demands for more anonymous service and for systems that will accept large sums. This is already beginning to happen. E-money developers are experimenting with fewer restrictions and higher value limits; in fact, some of the new products have no value limits at all. Most disturbingly, some systems will allow value to be accessed and transferred without the need for intervention by a regulated financial institution.

E-money could combine the anonymity of cash with the fluidity of digital communications. Transnational criminals could benefit tremendously from this development.

Undoubtedly, e-money will also play a role in other criminal offences and national security issues including tax evasion, fraud and counterfeiting. Moreover, this technology raises policy issues not directly related to criminal justice, issues such as the potential erosion of the tax base, loss of seignorage and privacy concerns.

Governments may need to address potential e-money laundering scenarios and modify their existing legislative, regulatory and enforcement practices. There may also be a need for greater international cooperation as the importance and the pervasiveness of digital currency grows.

BIBLIOGRAPHY

N.B.: Many separate working groups involving central bankers, finance and revenue departments, and regulatory and enforcement agencies have begun to define the scope of the problem (see bibliography). For example, Revenue Canada has created an *Advisory Committee on Electronic Commerce* consisting of representatives of Internet providers, financial institutions, tax professionals, computer experts, the provinces, and appropriate Federal Government Departments. They expect to have a working draft of their findings in early spring.

A Note About the Format of Internet Citations

Authors (contributor, corporate group and/or affiliation). "Title of the Document." *Title of Complete Work, Organization and/or Name of Site, if applicable.* Version or file number, if applicable. Date of last update, if applicable. URL location (date accessed).

Anderson, Christopher. "A Survey of Electronic Commerce: In Search of the Perfect Market." *The Economist*. http://www.economist.com/surveys/elcom/ec1.html (14 May 1997).

Angus, Ian. "Social Engineering for Phone Theft." *Technological Crime Bulletin*, 2, 2 (Sep. 1996): 4, 6.

Bass, Thomas A. "The Future of Money." *Wired Magazine*, 4, 10. Oct. 1996. http://www.wired.com/wired/4.10/features/wriston.html (28 May 1997).

Benyekhlef, Karim. "Les normes internationales de protection des données personnelles et l'autoroute de l'information." Jun. 1995. *Department of Justice Canada*. http://canada.justice.gc.ca/Conferences/Justice_AE/karim_fr.html (7 May 1997).

Birch, Dave & Neil McEvoy. "DIY Cash." *Wired Magazine*, 2 (Apr. 1996).

Birch, David G.W. "Column Five: Bye, Bye Banknotes." *Array Development*. http://www.arraydev.com/commerce/JIBC/9701-12.htm (28 May 1997).

Bortner, R. Mark. "Cyberlaundering: Anonymous Digital Cash and Money Laundering." 1996. *University of Miami Law School*. http://www.ovnet.com/~dckinder/documents/cyberlaunder.htm (17 Jun. 1997).

Boyles, David. "Testimony of David Boyles, Senior Vice President, New Business Ventures, Stored Value Group, and Smart Card Center of Excellence, American Express Travel Related Services, Inc. Before the Subcommittee on Domestic and International Monetary Policy of the Committee on Banking and Financial Services, U.S. House of

Representatives, June 11, 1996." *U.S. House of Representatives*. http://www.house.gov/castle/banking/dboyles.htm (28 May 1997).

Canada. Department of Justice Canada. *Developing a Legal Framework for an Information Age: Cybercrime and Electronic Democracy*. Strategic Planning and Special Projects Section, Department of Justice Canada. Ottawa: n.d.

Canada. Department of Justice Canada and Royal Canadian Mounted Police. *Investigation of Computer-Related Crime and Crimes Involving Information Technology*. Meeting of P-8 Senior Exerts Group on Transnational Organized Crime November 27-29, 1995. Ottawa: 1995.

Canada. Larson, Carole. National Security Directorate, Government of Canada. Memorandum entitled, "Internet Overview". 12 June 1997.

Channel Zero. "The Mondex Scenario: Transcript." Mar. 1997. http://www.channel-zero.com/screenings/ch0_cbc/show1/show1.htm (28 May 1997).

Chaum, David. "David Chaum's Testimony for US House of Representatives." *DigiCash*. 25 Jul. 1995. http://www.digicash.com/publish/testimony.html (15 May 1997).

Chaum, David. "Prepaid Smart Card Techniques: A Brief Introduction and Comparison." 1994. http://www.digicash.com/publish/cardcom.html (15 May 1997).

Cherneff, Ruth et al. "Smart Cards '97." *Shorenet*. 1 Nov. 1996. http://www1.shore.net/~bauster/cap/s-card/index.html (28 May 1997).

"Citicorp Suffers First "Cyberheist" as Regulators Show Alarm." *Money Laundering Alert*. 7, 1 (Oct. 1995): 9.

"Cleaning Up Dirty Money." *The Economist* (26 Jul. 1997), pp. 13-14.

Clinton, President William T. & Vice President Albert Gore Jr. "A Framework for Global Electronic Commerce. *The President's Information Infrastructure Task Force*. 1 Jul 1997. http://www.iitf.nist.gov/eleccomm/ecomm.htm (4 Sep. 1997).

Coale, Kristi. "EU Selling Swiss Army Smartcard Solution." *Wired News*. 1 Feb. 1997. http://www.wired.com/news/news/technology/story/1814.html (28 May 1997).

Committee on Payment and Settlement Systems. "Security of Electronic Money." *Bank for International Settlements*. http://www.bis.org/publ/cpss18.htm (21 May 1997).

Committee on Payment and Settlement Systems. "Security of Electronic Money (Executive Summary)." *Bank for International Settlements.* http://www.bis.org/publ/cpss18e.htm (12 Jun. 1997).

Committee on Payment and Settlement Systems and the Group of Computer Experts of the central banks of the Group of Ten countries. *Security of Electronic Money*, 1996.

Community Research and Development Information Service (CORDIS). "Conditional Access for Europe: Esprit Project EP 7023." *CORDIS.* 20 Mar. 1997.

"Computer crime continues to increase, Reported losses of over $100 million." *The Computer Security Institute.* 6 Mar. 1997. http://www.gocsi.com/preleas2.htm (28 Apr. 1997).

Cryptologic Inc. "Ecash Operations." http://www.cyptologic.com/index.html (9 Jul. 1997). http://www.cordis.lu/esprit/src/w4w19.htm (6 May 1997).

Denning, Dorothy E. "Encryption Policy and Market Trends." *Georgetown University, Department of Computer Science.* 11 Apr. 1997. http://guru.cosc.georgetown.edu/~denning/crypto/Trends.html (2 May 1997).

Donpa Ltd. "AVANT Electronic Purse in Finland." http://www.sci.fi/%7Edonpa/ep_finla.htm (28 May 1997).

Dorgan, Michael. "Netting Criminals: Financial Officials Try to Stop Illegal Activity from Taking Hold." *San Jose Mercury News.* 24 Apr. 1996. http://www.sjmercury.com/news/world/cyber423.htm (10 Jun. 1997).

Dugas, Sébastyen. "Un porte-feuille électronique Mondex, la monnaie du futur." *Direction informatique : Le journal des technologies de l'information.* 1996. http://www.direction-informatique.qc.ca/archives/96/04/mondex.html (28 May 1997).

Electronic Commerce News, 2, 25 (23 Jun. 1997).

Europay International. "Europay Launches the World's First Multi-Currency Electronic Purse 'Clip': Paves Way for Making Secure, Convenient, Low-value Purchases Internationally." 20 June 1996. http://www.europay.com/1996/ph6rtt0y.htm (28 May 1997).

Europay International. "The Use of Chip to Meet Consumer Demand: Europay International Members' Meeting, Seville, 1996." 20 June, 1996. http://www.europay.com/1996/ph6rtt1b.htm (28 May 1997).

Europay (Switzerland) SA. "CASH Resolves Problems with Small Change." 29 Jan. 1997. http://www.eurocard.ch/english/news/press1.html (28 May 1997).

European Committee on Crime Problems (CDPC). *Committee of Experts on Crime in Cyberspace (PC-CY). Problems of Legislation in the Area of Computer-related Crime.* Presented by Mr. M. Möhrenschlager (Ministry of Justice, Germany) at the International Symposium on Comparative Law, Recent Developments in Public Affairs. Istanbul, 1996.

Federal Reserve Bank of Dallas. "How Do We Pay?" First Quarter 1997. http://www.dallasfed.org/publications/fi/txt/fi_97_1q.html (28 May 1997).

First Virtual. "Buying Summary." http://www.fv.com/info/buyerintro.html (2 Jul. 1997).

Fried, Frank, Harris, Shriver & Jacobson. "Statement of Thomas P. Vartanian, Partner of Fried, Frank, Harris, Shriver & Jacobson, Before the Federal Deposit Insurance Corporation, Concerning Stored Value Cards and Electronic Payment Systems, September 12, 1996." http://ffhsj.com/bancmail/tpvtest.htm (28 May 1997).

Froomkin, A. Michael. "Flood Control on the Information Ocean: Living With Anonymity, Digital Cash, and Distributed Databases." *University of Miami Law School.* http://www.law.miami.edu/~froomkin/articles/oceanno.htm (31 Jul. 1997).

Froomkin, Michael. "The Unintended Consequences of E-Cash." *University of Miami Law School.* Version 1.2. 12 Mar. 1997. http://www.law.miami.edu/~froomkin/articles/cfp97.htm (31 Jul. 1997).

Frost, Mark. *A Brief Introduction to the Digitalization and Globalization of Money and Capital.* At Toronto, March 18-22, 1997.

"G7 Groups Frets Over Electronic Money Laudering." *The Nando Times.* 6 Feb. 1997. http://www.nando.net/newsroom/ntn/info/020697/info8_2320.html (26 May 1997).

Goldfinger, Charles of the Financial Issues Working Group (FIWG). "Electronic Money in the United States: Current Status, Prospects and Major Issues. Fact-finding Mission for the Financial Issues Working Group of the European Commission (Aug. 25 - Sep. 5, 1996)." *Information Society Project Office (ISPO).* 8 Jan. 1997. http://www.ispo.cec.be/infosoc/eleccom/elecmoney.html (6 May 1997).

Grigg, Ian. "Critique on the 1994 EU Report on Prepaid Cards." *Systemics Software Archive Document Library.* Nov.-Dec. 1996. http://www.systemics.com/docs/papers/1994_critique.html (28 May 1997).

Group of Ten. *Electronic Money: Consumer Protection, Law Enforcement, Supervisory and Cross Border Issues.* Report of the working party on electronic money. 1997. (Can be obtained electronically on Web site: http://www.bis.org).

Hallam-Baker, Dr. Phillip M. "Electronic Payment Schedules." *World Wide Web Consortium (W3C).* http://www.w3.org/Payments/roadmap.html (20 Aug. 1997).

Hannaford, Sgt. Craig. "Electronic Cash." *Technological Crime Bulletin*, 2, 2 (Sep. 1996): 5.

Harris, Holly. "La vie privée et l'autoroute de l'information." Jun. 1995. *Department of Justice Canada.* http://canada.justice.gc.ca/Conferences/Justice_AE/harris_fr.html (7 May 1997).

Hoenig, Thomas M. "The Evolution of the Payments System: A U.S. Perspective". *Economic Review, Federal Reserve Bank of Kansas City* (Third Quarter 1995), pp. 5-9.

Hughes, Sarah Jane. 1995a. " 'Cyberlaundering' Poses Threat to Controls." *Money Laundering Alert*, 6, 7 (Apr. 1995): 1, 6.

Hughes, Sarah Jane. 1995b. " 'Phantom' Cyberbanks Pose Laundering, Tax Evasion Threat." *Money Laundering Alert*, 6, 10 (July 1995): 4.

Info-sec.com. "German Law on Encrypted Telecommunications Examined." 28 Mar. 1997. http://www.info-sec.com/crypto/crypto_i.html-ssi (2 May 1997).

InterCasino. "InterCasino." http://www.intercasino.com/about/index.html (9 Jul. 1997).

International. Expert Group on "Misuse of International Data Networks". *Declaration of the Expert Group on "Misuse of International Data Networks" of the G7 Ministers of Science (Carnegie Group).* From First Meeting, Bonn 27-29 Nov. 1996. Version 1.0. 1997.

"Internet could become dirty money haven." *The Nando Times.* 14 Mar. 1996. http://www.nando.net/newsroom/ntn/info/031496/info3_11722.html (26 May 1997).

Jamieson, Cpl. Gordon. "Wireless Fraud: The Global Perspective." *Technological Crime Bulletin*, 2, 2 (Sep. 1996): 1, 6.

Johnson, James A. "Report on Organizations." *United States National Information Infrastructure Virtual Library.* Mar. 1997. http://nii.nist.gov/pubs/intl_org.html (6 May 1997).

McKay, Sam & Sari Kalin. "Will You Soon be Using Smart Cards for Electronic Payments?" *SunWorld*, 11, 3. 12 Mar. 1997. http://www.eimb.rssi.ru/sunworldonline/swol-03-1997/swol-03-att.html (22 May 1997).

McNeil, Mark. "Privacy up for Sale in a Buyer's Market: 'Electronic Trail' Left Behind as Credit Purchases Sell Out User." *The Hamilton Spectator*, 3 Apr. 1997. http://insight.dcss.mcmaster.ca/org/efc/pages/media/spectator.03apr97.html (22 May 1997).

Meister, Edgar. (Translation and Commentary by Kuner, Christopher Esq.). "Speech by Bundesbank Director Edgar Meister on Electronic Cash." 28 Nov. 1996. *Ourworld*. http://ourworld.compuserve.com/homepages/ckuner/meister.htm#meister (28 May 1997).

Mondex International. "Credit Union Central of Canada Joining Banks in Offering Mondex Electronic Cash." *Mondex International Press Releases*. 6 Feb. 1997. http://www.mondex.com/mondex/cgi-bin/show.pl?english+global&../english/documents/global/prel45243922.txt (28 May 1997).

Mondex International. "MasterCard International Completes 50 Per Cent Acquisition of Mondex International." *Mondex International Press Releases*. 23 Feb. 1997. http://www.mondex.com/mondex/cgi-bin/show.pl?english+global&../english/documents/global/prel61885785.txt (28 May 1997).

"Money Laundering: That Infernal Washing Machine." *The Economist* (26 Jul. 1997), pp. 19-21.

Morris, Stanly E. *Remarks by Stanley E. Morris, Director, Financial Crimes Enforcement Network, U.S. Department of the Treasury. To the Financial Services Forum, Financial Action Task Force*. Paris, France: 1996.

Muller, John D. "Selected U.S. Legal Issues in Issuance of Electronic Money." http://www.brobeck.com/docs/0497first.html (31 Jul. 1997).

OurWorld. "Report to the Council of the European Monetary Institute on Prepaid Cards by the Working Group on EU Payment Systems." May, 1994. http://ourworld.compuserve.com/homepages/ckuner/prepaid.htm (28 May 1997).

Piragroff, Donald & Annemieke Holhuis. "Les nids-de-poule de l'autoroute éléctronique : Crimes et abus." Jun. 1995. *Department of Justice Canada*. http://canada.justice.gc.ca/Conferences/Justice_AE/piragoff_fr.html (7 May 1997).

Porteous, Sam. "Organized Crime Impact Study - Highlights". Public Works and Government Services of Canada, 1998.

Porteous, Sam. *Transnational Organized Crime and E-cash*. Unclassified brief, CSIS. n.d.

Post, David G. "Anarcy, State, and the Internet: An Essay on Law-Making in Cyberspace (Article 3)." *Cornell Law School, Legal Information Institute*. 1995. http://www.law.cornell.edu/jol/post.html (1 May 1997).

Post, Prof. David G.. "Law of Cyberspace Seminar." *Cyberspace Law Institute*. Fall 1996. http://www.cli.org/cyberspace/index.html (1 May 1997).

Privacy International. "Privacy Internationals Mondex Complaint is Upheld: Electronic Cash is Anything but Anonymous." *Privacy International*. 21 Jun. 1997. http://www.privacy.org/pi/activities/mondex/mondex_release.html (28 May 1997).

Queau, Philippe. "Qui contrôlera la cyber-économie?" *Le Monde diplomatique*. Feb. 1995. http://www.monde-diplomatique.fr/md/1995/QUEAU/1160.html (27 Mar. 1997).

Quirk, Peter J. "Money Laundering: Muddying the Macroeconomy." *Finance & Development*. Mar. 1997. http://www.worldbank.org/fandd/english/abstract/0397/011a0397.htm (31 Jul. 1997).

"Recommendation No. R (95) 13 of the Committee of Ministers to Member States Concerning Problems of Criminal Procedure Law Connected with Information Technology." *Electronic Frontier Foundation*. 29 Sep. 1995. http://www.eff.org/pub/Global/Multinational/Privacy/ce_privacy_search_r95-13.recommendations (6 May 1997).

Reuters Ltd. "BankAmerica, VISA to Start Internet Test. *Yahoo! News*. 16 May 1997. http://www.yahoo.com/headlines/tech/stories/bankamerica_1.html (16 May 1997).

Richards, Scott. "Electronic Money/Internet Payment Systems." *Electronic Banking Resource Center*. http://www2.cob.ohio-state.edu/~richards/bankpay.htm (25 Jun. 1997).

Servida, Andrea. "Electronic Commerce - Security Related Projects (mostly in 4th FP)." *CORDIS*. 19 Mar. 1997. http://www.cordis.lu/esprit/src/w4w15.htm (6 May 1997).

"Shining a Light on Privacy." *Government Computer* (Apr. 1997), pp. 8, 10-11.

Sieber, Dr. Ulrich. *Research Proposal on Legal Aspects of Computer-Related Crime in the Information Society*. Würzburg: n.d.

Sieber, Prof. Dr. Ulrich. *EC-Research Project "Computer-related Crime" (COMCRIME), No. 1: General Information and Questionnaire for the Country Reports*. Würzburg: n.d.

Task Force on Stored-Value Cards. "A Commercial Lawyer's Take on the Electronic Purse: An Analysis of Commercial Law Issues Associated with Stored-Value Cards and Electronic Money." *The Business Lawyer*, 52, 2 (Feb. 1997): 653-727.

Taylor, Ian. "Licensing of Trusted Third Parties for the Provision of Encryption Services: Public Consultation Paper on Detailed Proposals for Legislation." *Department of Trade and Industry: Internet Services* (UK). Mar. 1997. http://dtiinfo1.dti.gov.uk/pubs (2 May 1997).

TD Bank. "Visa, Scotiabank and TD Bank Announce Canadian Trial of Reloadable Visa Cash Card." *TD Bank Press Releases*. 15 April 1997. http://www.tdbank.ca/tdbank/Press_Rel/apr15a97.htm (28 May 1997).

The Economist. "The Disappearing Taxpayer." *The Economist*. 1997. http://www.economist.com/issue/1-05-97/ld4660row.html (4 Jun. 1997).

The Economist. "Disappearing Taxes: The Tap Runs Dry." *The Economist*. 31 May 1997. http://www.economist.com/issue/31-05-97/sf0879.html (4 Jun. 1997).

The Economist. "Chipper, For Now." *The Economist*. 26 Apr. 1997. http://www.economist.com/issue/26-04-97/fn6691.html (28 May 1997).

The Economist. "Going for Olympic Gold Cards." *The Economist*. 30 Mar. 1997. http://www.economist.com/issue/30-03-96/fnl.html (28 May 1997).

The First Bank of Internet. "The First Bank of Internet." 20 Mar. 1995. http://www.cs.nps.navy.mil/curricula/tracks/security/homework/FBOI.txt (2 Jul. 1997).

Trend Monitor. "Beyond Money: The Implications of Electronic Cash and Virtual Banking." http://www.trendmon.demon.co.uk/eesa.htm (28 Jul. 1997).

United States. Democratic Staff of the Committee on Banking and Financial Services. "Connecting Consumers: Consumer Issues and Emerging Financial Technology." *House Committee on Banking and Financial Services. U.S. House of Representatives*. 21 Oct. 1996. http://www.house.gov/banking_democrats/consumers.html (31 Jul. 1997).

United States. Department of the Treasury. *An Introduction to Electronic Money Issues. Toward Electronic Money and Banking: The Role of Government*. Prepared for the United States Department of the Treasury Conference, 19-20 Sep. 1996, Washington, D.C.: 1996.

United States. Department of the Treasury. *Exploring the World of Cyberpayments: An Introductory Survey*, 1995.

United States. Department of the Treasury. "Money in Cyberspace: Frequenty Asked Questions." 3 Feb. 1997. http://www.treas.gov/treasury/bureaus/fincen/cybpage.html (18 Jun. 1997).

United States. Office of the Comptroller of the Currency, U.S. Department of the Treasury. "Toward Electronic Money & Banking: The Role of Government. A Conference Sponsored by the United States Department of the Treasury. Washington, DC, Sep. 19-20, 1996." *Office of the Comptroller of the Currency.* http://www.occ.treas.gov/emoney.htm (11 Mar. 1997).

United States. Subcommittee on Domestic and International Monetary Policy, U.S. House of Representatives. "Submission to the US House of Representatives by Mondex on 'The Future of Money', June 11th 1996." *U.S. House of Representatives.* http://www.house.gov/castle/banking/jones.htm (28 May 1997).

United States. Subcommittee on Domestic and International Monetary Policy, U.S. House of Representatives. "Testimony of Professor James L. Brown, Director, Center for Consumer Affairs, University of Wisconsin, Milwaukee Before the Subcommittee on Domestic and International Monetary Policy of the Committee on Banking and Financial Services, US House of Representatives. Regarding Implications of Electronic Banking and Commerce." *U.S. House of Representatives.* 7 Mar. 1997. http://www.house.gov/castle/banking/brown3.htm (31 Jul. 1997).

van der Wielen, Henry. "Electronic Money: A European Perspective." *Systemics Software Archive Document Library.* 4 Feb. 1997. http://www.systemics.com/docs/papers/EU_perspective.html (31 Jul. 1997).

Van Hove, Leo. "A Selected Bibliography on Electronic Purses." *Leo Van Hove - bibliography on electronic purses.* http://cfec.vub.ac.be/cfec/purses.htm (28 May 1997).

Wahlert, Glenn. "Money Laundering, the Perils of Cyberpayments." *Technological Crime Bulletin*, 2 2 (Sep. 1996): 2-3.

***** *other sources may have been used***

APPENDIX I:
HOW E-MONEY WORKS
(applies to most current e-money systems)

E-money is a generic name given to the concept of currency which is digitally signed by an issuing institution through a private encryption key and is transmitted to an individual. It can then be negotiated, electronically, with others as payment for goods and services anywhere in the world.

- Via the Internet, a home PC user requests e-money by logging onto his/her bank and authenticating ownership of his/her account.
- Once ownership is confirmed, the user submits a request along with a random encryption key in a secure digital envelope.
- The bank the signs the envelope with its signature (thus authenticating the E-money for potential recipients) and it is returned to the user.
- The user can now download the digital money onto a smart card through an ATM-like peripheral or he/she can transfer/spend the money over the Internet with the same reach as an e-mail message.
- Recipients simply copy the E-money and have their computer add their own account ID to it. It can either be stored on a smart card or transferred to their bank.

Other Electronic Money Technology

E-money is on-line currency that can be exchanged between two parties without the need for a third party to complete the transaction. Stored value cards are a different technology that, in comparison to e-money, are only stored pre-paid money.

Stored value cards are described as:
"A prepaid smart card contains stored value which the person holding it can spend at retailers. After accepting stored value from cards, retailers are periodically reimbursed with actual money by system providers. A system provider receives money in advance from people and stores corresponding value onto their cards. During each of these three kinds of transactions, secured data representing value is exchanged for actual money or for goods and services" (Chaum, 1994).

Examples of simple stored value cards that are currently being used include: phone cards; university cash cards; and ski resort payment systems. During the Atlantic Olympics a more advanced version of this type of card was distributed to over 300,00 individuals.

There are four basic types of technology:

memory cards: these cards are for storage only (they cannot compute). They have some software for PIN numbers.

shared-key cards: keys in a computer chip within the card let the card communicate with any other device with the same keys (Chaum, 1994).

signature-transporting cards: these cards are similar to shared-key cards, but have slightly different software. Each card stores a digital signature. Each time the card is used, the system provider fills in the digital signature, like filling in a blank cheque.

signature-creating cards: these cards are the same as signature-transporting cards; however, the computer chip within each card is capable of making digital signatures. Therefore, the signature is made on each card, not by the system provider.

APPENDIX II:
CRYPTOGRAPHY AND ELECTRONIC COMMERCE

Cryptography (encryption) is particularly important to the growth of electronic commerce because it provides the means to ensure the authenticity, integrity and privacy of transactions and communications, providing the necessary security for the digital world.

It is the process of substituting numbers and letters for other numbers and letters, making the message or communications unreadable. These substitution codes are hidden in keys which can then be used to encrypt messages and communications and decrypt them once they are encrypted.

Criminals and terrorists can use cryptography with relative ease to thwart the legally mandated information-gathering abilities of law enforcement and security agencies. For example, evidence that has been encrypted is unreadable unless it can be decrypted. The inability to decrypt could well have a severe impact on the prevention, detection, investigation, and prosecution of crime, as well on Canada's ability to monitor security threats to Canadians. It is for these reasons that arguments are made in favour of reasonable limits on the production, export, import and use of cryptography.

(For a detailed discussion on cryptography please refer to the discussion paper *Cryptography and Electronic Commerce: Setting a Policy Framework for Canada*, Industry Canada, February 1998.)

APPENDIX III:
PAYMENT SYSTEMS ATTRIBUTES
SOME SIMPLIFIED GENERALIZATIONS FOR DISCUSSION

Current Payment Systems	Cyberpayments System
• High degree of central bank control	• Various national views re: control
• Highly structured supervision/regulation	• Highly technical, yet to be designed
• Large legal and policy literature	• Reg E to small degree
• Body of examining and Customs mechanisms	• Monitoring technology unavailable
• Physical means of payments-checks, currency	• Intangible electronic analogs
• Huge infrastructure established worldwide	• Downsized, computer based
• Relatively labour intensive	• Relatively capital intensive
• High value infrastructure-brick and mortar	• Low cost decentralized facilities
• Bank-dominated wire transfers	• Personal computer transfers
• Check-dominated consumer payments	• Cybercurrency-dominated
• Velocity of money is low	• Velocity of money is high
• Bank-dominated intermediaries	• Non-traditional intermediaries
• Clearing mechanism required	• Clearing requirement reduced
• Transportation-couriers, land, sea, air	• Telecommunications
• Worldwide use of US currency	• Easy currency exchange/one currency
• Serial numbers and bank records	• Encrypted messages
• Significant statistical data collection	• No methodology for Ms statistics
• Economic national borders	• No borders, effectively

- Defined jurisdictions
- Generally non-refutable, standard methods of validation
- Fungible
- Authentication, established structure to verify authenticity

- Overlapping, unknown jurisdictions
- Evolving methods of transaction verification
- System specific convertibility to cash
- Undetermined, system specific may involve third party

APPENDIX IV: SURVEY OF POLICIES TOWARD ELECTRONIC MONEY IN THE G-10 COUNTRIES

Survey of Policies Toward Electronic Money in the G-10 Countries

Country	Fraud, loss, theft, disputes	Disclosure requirements
Belgium	General applicability of civil code and rules for credit institutions. Voluntary banking association ombudsman program for settling disputes may be applicable to electronic money.	General applicability of civil code and rules for credit institutions.
Canada	General applicability of civil code and rules for credit institutions. Banking industry ombudsman. Industry association developing standards on security against fraud and theft for electronic money for stored-value cards.	Disclosures required for all service charges related to bank and trust and loan company accounts, including charges for electronic funds transfers from deposit accounts. Disclosure is also required regarding consumer rights and obligations respecting credit cards.
France	General applicability of civil code (errors and disputes) and rules for credit institutions (currently applies to loss or theft of checks and credit cards).	General applicability of civil code and rules for credit institutions.
Germany	General applicability of civil code. Ombudsman program.	General applicability of civil code and rules for credit institutions.
Italy	General applicability of civil code and 1993 banking law. Banking industry self-regulatory code applicable to electronic money schemes. Banking industry ombudsman to settle disputes.	Regulatory authorities plan to require broad disclosure of information to consumers.
Japan	General applicability of civil code and rules for credit institutions. Financial and technology entities have developed technical standards to prevent fraud, loss, theft for computer systems of financial institutions.	General applicability of civil code and rules for credit institutions. Prepaid Card Law requires that any limits or term and location of use must be disclosed on the card.
Netherlands	Dispute resolution procedures of courts and banking industry committee apply to electronic money. Banking industry Code of Best Practices on consumer protection. Dutch government recognises self-regulatory measures.	General applicability of civil code and rules for credit institutions.
Sweden	General applicability of civil code and rules for credit institutions.	General applicability of civil code and rules for credit institutions.
Switzerland	General applicability of civil and penal codes.	General applicability of civil code.
United	Dispute resolution and unfair terms addressed in Fair	General provisions of the Code of

Kingdom	Trading Act, Unfair Terms in Consumer Contracts Act. Code of Banking Practice covers loss and errors where banks or building societies are involved. Voluntary banking ombudsman and statutory building societies ombudsman.	Banking Practice apply to banks and building societies.
United States	Applicability general commercial law. Applicability of the Electronic Fund Transfer Act to stored-value products under review by the Federal Reserve.	Applicability of disclosure of Electronic Fund Transfer Act to stored-value products under review by the Federal Reserve. Office of the Comptroller of the Currency has issued guidance to national banks.

Country	**Prudential requirements for issuers**	**Examinations, internal controls, and information systems security**
Belgium	For credit institutions as for other banking activities.	Procedures applicable to credit institutions. National Bank of Belgium collects statistical information from electronic money system operators twice each year. It has conducted an informal audit of the electronic money scheme.
Canada	For regulated financial institutions, existing legislation and regulatory requirements apply, including capital requirements.	Procedures applicable to regulated financial institutions.
France	Regular banking regulations.	Same procedures for credit institutions (on-site examinations, internal controls, information security audits).
Germany	Standard minimum capital, solvency and liquidity requirements for credit institutions that take deposits and make loans. Modified requirements possible for institutions that only issue electronic money.	Credit institutions submit monthly reports to the Bundesbank and annual accounts, annual reports, and auditor reports to the FBAs and Bundesbank.
Italy	Same as for other banking activities.	Standard examination and reporting for credit institutions. Electronic money schemes currently subject to off-site controls. The Bank of Italy is considering introduction of specific information systems security and internal control requirements.
Japan	Credit institutions subject to requirements of Banking Law. Issuers covered by the Prepaid Card Law must deposit funds with the Depository Office of not less than 50% of unused balances of cards issued.	Credit institutions subject to regular reporting requirements and examinations. Issuers under the Prepaid Card Law subject to regular reporting requirements and, for 3-party issuers, subject to examinations.
Netherlands	Issuers must comply with all requirements of the Act on the Supervision of Credit System, including liquidity and capital adequacy	Same procedures for credit institutions, including qualifications and management and system operator to fulfil security and integrity requirements of the electronic money scheme.

	requirements.	On-site and off-site examinations and external audits.
Sweden	Standard banking laws and regulatory procedures apply to banks.	Standard banking requirements apply. On-site and off-site examinations and external audits.
Switzerland	Swiss Banking Law specifies financial requirements for banks, which are supervised by the Federal Banking Commission.	External auditor reports for banks. Swiss Code of Obligation subjects other companies to examination procedures in order to fulfil common industry standards.
United Kingdom	Standard banking laws and regulatory procedures apply to banks.	Banks and building societies must show evidence of a realistic business plan and adequate systems and controls.
United States	No special financial requirements for banks issuing electronic money. Some states prescribe investment standards for non-bank money transmitters; applicability to electronic money issuers unclear.	On-site, generally annual examinations for banks, covering information systems security, internal controls, etc. Examination authority for bank holding companies and subsidiaries of banks. Some states examine non-bank money transmitters or have other requirements.

Country	**Licensing**
Belgium	Currently, no legal restriction on issuance of electronic money. Only credit institutions have issued electronic money to date. No special authorisation needed for those institutions to issue electronic money.
Canada	No current prohibition on electronic money issuance by non-financial institutions (only regulated deposit-taking financial institutions have issued electronic money to date). Approval may be required for a financial institution to establish a subsidiary.
France	French Banking Act requires electronic money issuers to be credit institutions, with the exception of limited-purpose prepaid cards. No special authorisation needed for credit institutions to issue electronic money but any scheme must be submitted to the Bank of France.
Germany	Electronic money issuers must be credit institutions, except for limited-purpose (2-party) prepaid cards. No special authorisation needed for full-scale credit institutions to issue prepaid cards or network electronic money. A general-purpose prepaid card issuer may be exempted from the licensing requirements at the discretion of the Federal Bank Supervisory Office.
Italy	Issuers of mullet-purpose electronic money must be credit institutions. No special authorisation needed for credit institutions.
Japan	Restriction of issuance of electronic money redeemable with cash to credit institutions under review. Under the Prepaid Card Law, 2-party issuers (issuer and merchant are the same) must notify the Ministry of Finance; issuers of 3-party (other than 2-party type) cards must register with the Ministry of Finance.
Netherlands	Issuers of electronic money are considered credit institutions, which have to obtain authorisation

	from the Netherlands Bank. Exceptions can be made for small-scale electronic money schemes.
	Entities involved in implementing an electronic money scheme, but not issuing electronic money themselves, are not considered to be credit institutions.
Sweden	Currently no restrictions on issuance of electronic money.
	No special authorisation needed for banks.
	To date, only banks and credit institutions have issued electronic money.
Switzerland	Authorities have not delivered an opinion on issuance of electronic money. To date, only banks and the Swiss Postal Office participate in general-purpose electronic money schemes. In the opinion of the Federal Banking Commission, issuance of e-money is linked to a professional offer in public to accept clients' assets, which is restricted to banks.
	Proposed money laundering laws will require electronic money issuers to belong to a self-regulatory organisation or be licensed by a special government entity.
United Kingdom	Banks subject to general authorisation in Banking Act, or building societies in the Building Societies Act.
	Non-bank issuers of electronic money schemes that do not have characteristics of deposit taking would not require authorisation. Non-banks involved with electronic money schemes that do have the characteristics of deposit taking would have either to apply for authorisation themselves, or enter into a joint venture with an authorised institution, which would be responsible for the deposit taking element.
United States	No special authorisation needed for banks to issue electronic money products. Authorisation may be required for a bank to invest in a separate entity to conduct such activities.
	State money transmitter laws may require non-depository institutions that issue electronic money products to be licensed.

Country	**Anti-money laundering measures**
Belgium	Anti- money laundering laws applicable to credit institutions.
Canada	Measures apply if issuer is a regulated financial institution.
France	Anti- money laundering laws and regulations applicable to credit institutions.
Germany	Anti- money laundering laws and regulations applicable to credit institutions.
Italy	Anti- money laundering laws and regulations applicable to credit institutions.
Japan	Anti- money laundering laws and regulations applicable to credit institutions and other institutions.

Netherlands	Anti- money laundering law applies, including "know-your-customer" and reporting of unusual transactions.
Sweden	Anti- money laundering laws and regulations applicable to credit institutions.
Switzerland	Proposed law on money laundering will be applicable to all financial intermediaries, including electronic money issuers; the proposed law requires that financial intermediaries provide any kind of information that will allow the reconstruction of transactions.
United Kingdom	Money Laundering Regulations of 1993 apply to electronic money. Requirements for reporting suspicious transactions and ability to supply an audit trail.
United States	Anti- money laundering laws and regulations applicable to banks and other institutions. Applicability to electronic money products under review.

Country	Deposit insurance or other guarantees	Privacy
Belgium	Applicability of deposit insurance scheme to electronic money products is under review.	Belgian law incorporates the EC Directive on Protector of Personal Data
Canada	Applicability of deposit insurance scheme to electronic money products is under review.	Regulations to be introduced in 1997 for federally regulated financial institutions. Broad privacy legislation at federal level to be developed by 2000. Quebec has adopted privacy legislation applicable to the private sector. Financial institutions to adopt the Canadian Standards Association's privacy code in 1997. Canadian Payments Association imposes general privacy obligations.
France	Deposit insurance scheme applies to electronic money.	General applicability of civil code. Applicability of French banking law. Consent of consumer required for transfer of personal information.
Germany	Rules for credit institutions.	General applicability of civil code.
Italy	Deposit insurance scheme applies to electronic money. Bearer cards are excluded.	EC Directive recently implemented by Parliament.
Japan	Applicability of deposit insurance to electronic money under review. Under the Prepaid Card Law, card holders have priority claim on funds issuers must deposit with the Depository Office.	Industry groups have issued detailed guidelines on consumer privacy for financial institutions.

Netherlands	Applicability of deposit insurance scheme to electronic money under consideration. Banks participating in electronic money systems have developed loss-sharing plan in the event of insolvency of one of the group.	Dutch Act on the Registration of Personal Data and EC Directive apply to electronic money.
Sweden	Deposit Guarantee Board has determined that the deposit guarantee scheme is applicable to existing prepaid cards issued by banks.	General laws on privacy applicable to banks and other credit institutions.
Switzerland	Banks participating in electronic money systems have developed loss-sharing plan in the event of the insolvency of one of the group.	General applicability of civil code.
United Kingdom	Dispute resolution and unfair terms addressed in Fair Trading Act, Unfair Terms in Consumer Contracts Act. Code of Banking Practice covers loss and errors where banks or building societies are involved. Voluntary banking ombudsman and statutory building societies ombudsman.	General provisions of the Code of Banking Practice apply to banks and building societies.
United States	Applicability general commercial law. Applicability of the Electronic Fund Transfer Act to stored-value products under review by the Federal Reserve.	Applicability of disclosure of Electronic Fund Transfer Act to stored-value products under review by the Federal Reserve. Office of the Comptroller of the Currency has issued guidance to national banks.

Revised FATF Recommendations

Introduction

1. The Financial Action Task Force on Money Laundering (FATF) is an inter-governmental body whose purpose is the development and promotion of policies to combat money laundering - the processing of criminal proceeds in order to disguise their illegal origin. These policies aim to prevent such proceeds from being utilized in future criminal activities and from affecting legitimate economic activities.

2. The FATF currently consists of 26 (Reference in this document to "countries" should be taken to apply equally to "territories" or "jurisdictions". The twenty six FATF member countries and governments are: Australia, Austria, Belgium, Canada, Denmark, Finland, France, Germany, Greece, Hong Kong, Iceland, Ireland, Italy, Japan, Luxembourg, the Kingdom of the Netherlands, New Zealand. Norway, Portugal, Singapore, Spain, Sweden, Switzerland, Turkey, United Kingdom, and the United States) countries and two international organizations. (The two international organizations are: the European Commission and the Gulf Cooperation Council.) Its membership includes the major financial center countries of Europe, North America and Asia. It is a multidisciplinary body - as is essential in dealing with money laundering, - bringing together the policy-making power of legal, financial and law enforcement experts.

3. This need to cover all relevant aspects of the fight against money laundering is reflected in the scope of the forty FATF Recommendations - the measures which the Task Force have agreed to implement and which all countries are encouraged to adopt. The Recommendations were originally drawn up in 1990. In 1996 the forty Recommendations were revised to take into account the experience gained over the last six years and to reflect the changes which have occurred in the money-laundering problem. (During the period 1990 to 1995, the FATF also elaborated various Interpretative Notes that are designed to clarify the application of specific Recommendations. Some of these Interpretative Notes have been updated in the Stocktaking Review to reflect changes in the Recommendations.)

4. These forty Recommendations set out the basic framework for anti-money laundering efforts and they are designed to be of universal application. They cover the criminal justice system and law enforcement; the financial system and its regulation, and international cooperation.

5. It was recognized from the outset of the FATF that countries have diverse legal and financial systems and so all cannot take identical measures. The Recommendations are therefore the principles for action in this field, for countries to implement according to their particular circumstances and constitutional frameworks allowing countries a measure of flexibility rather than prescribing every detail. The measures are not particularly complex or difficult, provided

there is the political will to act. Nor do they compromise the freedom to engage in legitimate transactions or threaten economic development.

6. FATF countries are clearly committed to accept the discipline of being subjected to multilateral surveillance and peer review. All member countries have their implementation of the 40 Recommendations monitored through a two-pronged approach: an annual self-assessment exercise and the more detailed mutual evaluation process under which each member country is subject to an on-site examination. In addition, the FATF carries out cross-country reviews of measures taken to implement particular Recommendations.

7. These measures are essential for the creation of an effective anti-money laundering framework,

FORTY RECOMMENDATIONS OF THE TASK FORCE

A. GENERAL FRAMEWORK OF THE RECOMMENDATIONS

1. Each country should take immediate steps to ratify and to implement fully, the 1988 United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances (the Vienna Convention).

2. Financial institution secrecy laws should be conceived so as not to inhibit implementation of these recommendations.

3. An effective money laundering enforcement program should include increased multilateral cooperation and mutual legal assistance in money laundering investigations and prosecutions and extradition in money laundering cases, where possible.

B. ROLE OF NATIONAL LEGAL SYSTEMS IN COMBATTING MONEY LAUNDERING

Scope of the Criminal Offense of Money Laundering

4. Each country should take such measures as may be necessary, including legislative ones, to enable it to criminalize money laundering as set forth in the Vienna Convention. Each country should extend the offense of drug money laundering to one based on serious offenses. Each country would determine which serious crimes would be designated as money laundering predicate offenses.

5. As provided in the Vienna Convention, the offense of money laundering should apply at least to knowing money laundering activity, including the concept that knowledge may be inferred from objective factual circumstances.

6. Where possible, corporations themselves - not only their employees - should be subject to criminal liability.

Provisional Measures and Confiscation

7. Countries should adopt measures similar to those set forth in the Vienna Convention, as may be necessary, including legislative ones, to enable their competent authorities to confiscate property laundered, proceeds from, instrumentalities used in or intended for use in the commission of any money laundering offense, or property of corresponding value, without prejudicing the rights of bona fide third parties.

Such measures should include the authority to: 1) identify, trace and evaluate property which is subject to confiscation; 2) carry out provisional measures, such as freezing and seizing, to prevent any dealing, transfer or disposal of such property; and 3) take any appropriate investigative measures.

In addition to confiscation and criminal sanctions, countries also should consider monetary and civil penalties, and/or proceedings including civil proceedings, to void contracts entered into by parties, where parties knew or should have known that as a result of the contract, the State would be prejudiced in its ability to recover financial claims, e.g., through confiscation or collection of fines and penalties.

C. ROLE OF THE FINANCIAL SYSTEM IN COMBATING MONEY LAUNDERING

8. Recommendations 10 to 29 should apply not only to banks, but also to non-bank financial institutions. Even for those non-bank financial institutions which are not subject to a formal prudential supervisory regime in all countries, for example bureaux de change, governments should ensure that these institutions are subject to the same anti-money laundering laws or regulations as all other financial institutions and that these laws or regulations are implemented effectively.

9. The appropriate national authorities should consider applying Recommendations 10 to 21 and 23 to the conduct of financial activities as a commercial undertaking by businesses or professions which are not financial institutions, where such conduct is allowed or not prohibited. Financial activities include, but are not limited to, those listed in the attached annex. It is left to each country to decide whether special situations should be defined where the application of anti-money laundering measures is not necessary, for example, when a financial activity is carried out on an occasional or limited basis.

Customer Identification and Record-keeping Rules

10. Financial institutions should not keep anonymous accounts or accounts in obviously fictitious names: they should be required (by law, by regulations, by agreements between supervisory authorities and financial institutions or by self-regulatory agreements among financial institutions) to identify, on the basis of an official or other reliable identifying document, and record the identity of their clients, either occasional or usual, when establishing business relations or conducting transactions (in particular opening of accounts or passbooks, entering into fiduciary transactions, renting of safe deposit boxes, performing large cash transactions).

In order to fulfill identification requirements concerning legal entities, financial institutions should, when necessary, take measures:

(i) to verify the legal existence and structure of the customer by obtaining either from a public register or from the customer or both, proof of incorporation, including information concerning the customer's name, legal form, address, directors and provisions regulating the power to bind the entity.

(ii) to verify that any person purporting to act an behalf of the customer is so authorized and identify that person.

11. Financial institutions should take reasonable measures to obtain information about the true identity of the persons on whose behalf an account is opened or a transaction conducted if there are any doubts as to whether these clients or customers are acting an their own behalf, for example, in the case of domiciliary companies (i.e. institutions, corporations, foundations, trusts, etc. that do not conduct any commercial or manufacturing business or any other form of commercial operation in the country where their registered office is located).

12. Financial institutions should maintain for at least five years, all necessary records on transactions, both domestic or international, to enable them to comply swiftly with information requests from the competent authorities. Such records must be sufficient to permit reconstruction of individual transactions (including the amounts and types of currency involved if any) so as to provide, if necessary, evidence for prosecution of criminal behavior.

Financial institutions should keep records on customer identification (e.g., copies or records of official identification documents like passports, identity cards, driving licenses or similar documents), account files and business correspondence for at least five years after the account is closed.

These documents should be available to domestic competent authorities in the context of relevant criminal prosecutions and investigations.

13. Countries should pay special attention to money laundering threats inherent in new or developing technologies that might favor anonymity, and take measures, if needed, to prevent their use in money laundering schemes.

Increased Diligence of Financial Institutions

14. Financial institutions should pay special attention to all complex, unusual large transactions, and all unusual patterns of transactions, which have no apparent economic or visible lawful purpose. The background and purpose of such transactions should, as soon as possible, be examined, the findings established in writing, and made available to help supervisors, auditors and law enforcement.

15. If financial institutions suspect that funds stem from a criminal activity, they should be required to report promptly their suspicions to the competent authorities.

16. Financial institutions, their directors, officers and employees should be protected by legal provisions from criminal or civil liability for breach of any restriction an disclosure of information imposed by contract or by any legislative, regulatory or administrative provision, if they report their suspicions in good faith to the competent authorities, even if they did not know precisely what the underlying criminal activity was, and regardless of whether illegal activity actually occurred.

17. Financial institutions, their directors, officers and employees, should not, or, where appropriate, should not be allowed to, warn their customers when information relating to them is being reported to the competent authorities.

18. Financial institutions reporting their suspicions should comply with instructions from the competent authorities.

19. Financial institutions should develop programs against money laundering. These programs should include, as a minimum:

(i) the development of internal policies, procedures and controls, including the designation of compliance officers at management level, and adequate screening procedures to ensure high standards when hiring employees;

(ii) an ongoing employee training program;

(iii) an audit function to test the system.

Measures to Cope with the Problem of Countries with No or Insufficient Anti-Money Laundering Measures

20. Financial institutions should ensure that the principles mentioned above are also applied to branches and majority owned subsidiaries located abroad, especially in countries which do not or insufficiently apply these Recommendations, to the extent that local applicable laws and regulations permit. When local applicable laws and regulations prohibit this implementation, competent authorities in the country of the mother institution should be informed by the financial institutions that they cannot apply these Recommendations.

21. Financial institutions should give special attention to business relations and transactions with persons, including companies and financial institutions, from countries which do not or insufficiently apply these Recommendations. Whenever these actions have no apparent economic or visible lawful purpose, their background and purpose should, as far as possible, be examined, the findings established in writing, and be available to help supervisors, auditors and law enforcement agencies.

Other Measures to Avoid Money Laundering

22. Countries should consider implementing feasible measures to detect or monitor the physical cross-border transportation of cash and bearer negotiable instruments, subject to strict safeguards to ensure proper use of information and without impeding in any way the freedom of capital movements.

23. Countries should consider the feasibility and utility of a system where banks and other financial institutions and intermediaries would report all domestic and international currency transactions above a fixed amount, to a national central agency with a computerized data base, available to competent authorities for use in money laundering cases, subject to strict safeguards to ensure proper use of the information.

24. Countries should further encourage in general the development of modern and secure techniques of money management, including increased use of checks, payment cards, direct deposit of salary checks, and book entry recording of securities. as a means to encourage the replacement of cash transfers.

25. Countries should take notice of the potential for abuse of shell corporations by money launderers and should consider whether additional measures are required to prevent unlawful use of such entities.

Implementation, and Role of Regulatory and other Administrative Authorities

26. The competent authorities supervising banks or other financial institutions or intermediaries, or other competent authorities, should ensure that the supervised institutions have adequate programs to guard against money laundering. These authorities should cooperate and

lend expertise spontaneously or on request with other domestic judicial or law enforcement authorities in money laundering investigations and prosecutions.

27. Competent authorities should be designated to ensure an effective implementation of all these Recommendations, through administrative supervision and regulation, in other professions dealing with cash as defined by each country.

28. The competent authorities should establish guidelines which will assist financial institutions in detecting suspicious patterns of behavior by their customers. It is understood that such guidelines must develop over time, and will never be exhaustive. It is further understood that such guidelines will primarily serve as an educational tool for financial institutions' personnel.

29. The competent authorities regulating or supervising financial institutions should take the necessary legal or regulatory measures to guard against control or acquisition of a significant participation in financial institutions by criminals or their confederates.

STRENGTHENING OF INTERNATIONAL COOPERATION

Administrative Cooperation / Exchange of general information

30. National administrations should consider recording, at least in the aggregate, international flows of cash in whatever currency, so that estimates can be made of cash flows and reflows from various sources abroad, when this is combined with central bank information. Such information should be made available to the International Monetary Fund and the Bank for International Settlements to facilitate international studies.

31. International competent authorities, perhaps Interpol and the World Customs Organization, should be given responsibility for gathering and disseminating information to competent authorities about the latest developments in money laundering and money laundering techniques. Central banks and bank regulators could do the same on their network. National authorities in various spheres, in consultation with trade associations, could then disseminate this to financial institutions in individual countries.

Exchange of information relating to suspicious transactions

32. Each country should make efforts to improve a spontaneous or "upon request" international information exchange relating to suspicious transactions, persons and corporations involved in those transactions between competent authorities. Strict safeguards should be established to ensure that this exchange of information is consistent with national and international provisions on privacy and data protection.

Other forms of Cooperation

Basis and means for cooperation in confiscation, mutual assistance and extradition

33. Countries should try to ensure, on a bilateral or multilateral basis, that different knowledge standards in national definitions i.e. different standards concerning the intentional element of the infraction - do not affect the ability or willingness of countries to provide each other with mutual legal assistance.

34. International cooperation should be supported by a network of bilateral and multilateral agreements and arrangements based on generally shared legal concepts with the aim of providing practical measures to affect the widest possible range of mutual assistance.

35. Countries should be encouraged to ratify and implement relevant international conventions on money laundering such as the 1990 Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime.

Focus of improved mutual assistance on money laundering issues

36. Cooperative investigations among countries' appropriate competent authorities should be encouraged. One valid and effective investigative technique in this respect is controlled delivery related to assets known or suspected to be the proceeds of crime. Countries are encouraged to support this technique, where possible.

37. There should be procedures for mutual assistance in criminal matters regarding the use of compulsory measures including the production of records by financial institutions and other persons, the search of persons and premises, seizure and obtaining of evidence for use in money laundering investigations and prosecutions and in related actions in foreign jurisdictions.

38. There should be authority to take expeditious action in response to requests by foreign countries to identify, freeze, seize and confiscate proceeds or other property of corresponding value to such proceeds, based on money laundering or the crimes underlying the laundering activity. There should also be arrangements for coordinating seizure and confiscation proceedings which may include the sharing of confiscated assets.

39. To avoid conflicts of jurisdiction, consideration should be given to devising and applying mechanisms for determining the best venue for prosecution of defendants in the interests of justice in cases that are subject to prosecution in more than one country. Similarly, there should be arrangements for coordinating seizure and confiscation proceedings which may include the sharing of confiscated assets.

40. Countries should have procedures in place to extradite, where possible, individuals charged with a money laundering offense or related offenses. With respect to its national legal system, each country should recognize money laundering as an extraditable offense. Subject to their legal frameworks, countries may consider simplifying extradition by allowing direct transmission of extradition requests between appropriate ministries, extraditing persons based

only on warrants of arrests or judgments, extraditing their nationals, and/or introducing a simplified extradition of consenting persons who waive formal extradition proceedings.

Annex to Recommendation 9: List of Financial Activities undertaken by business or professions which are not financial institutions

1. Acceptance of deposits and other repayable funds from the public.

2. Lending (including inter alia: consumer credit; mortgage credit; factoring, with or without recourse; finance of commercial transactions (including forfeiting)).

3. Financial leasing.

4. Money transmission services.

5. Issuing and managing means of payment (e.g., credit and debit cards, cheques, traveller's cheques and banker's drafts…)

6. Financial guarantees and commitments.

7. Trading for account of customers (spot, forward, swaps, futures, options ...) in:

(a) money market instruments (cheques, bills, CDs, etc.)

(b) foreign exchange;

(c) exchange, interest rate and index instruments;

(d) transferable securities;

(e) commodity futures trading.

8. Participation in securities issues and the provision of financial services related to such issues.

9. Individual and collective portfolio management.

10. Safekeeping and administration of cash or liquid securities on behalf of clients.

11. Life insurance and other investment related insurance.

12. Money changing.